スピングラス理論に基づく情報通信研究の新展開 : 誤り訂正符号を中心に(情報統計力学,第46回物性若手夏の学校(2001年度)(その1),講義ノート)

AUTHOR(S):

樺島, 祥介

スピングラス理論に基づく情報通信研究の新展開

— 誤り訂正符号を中心に —

東京工業大学 知能システム科学専攻　樺島祥介[1]

1　はじめに

強磁性体と反強磁性体から作られた合金の磁性を明らかにする目的からはじまったスピングラス理論であるが，80年代後半より情報科学や数理工学への応用が活発化している．本稿では特に最近注目されている情報通信分野へのスピングラス理論の応用に関して述べたい．

ただし，スピングラス自体一般的にはそれほど馴染み深い話題ではない．そこで，まずはスピングラス理論についての入門的な解説から始めることにしよう．

2　スピングラスの平均場理論

2.1　SK模型

ハミルトニアン

$$\mathcal{H}(\boldsymbol{S}|\left\{J_{\langle ij\rangle}\right\}) = -\sum_{\langle ij\rangle} J_{\langle ij\rangle} S_i S_j \tag{1}$$

で与えられるイジングスピン系 $S_i = \pm 1$ を考える．全てのスピン対 $\langle ij\rangle$ について $J_{\langle ij\rangle} > 0$ なら強磁性体，$J_{\langle ij\rangle} < 0$ なら反強磁性体である．

さて，金属では合金といって複数の物質を融解し冷やし固めることで性質の違った材料を作ることが出来る．この際，融解し液状化した合金を急速に冷却すると原子レベルで物質が混ざりあったまま固化する．ここでもし物質の組合せが鉄と金のように強磁性体と反強磁性体であったとすると，このように作られた合金におけるスピンの相互作用の性質は隣接する原子が強磁性体か反強磁性体かによってがらりと変わることになる．このような系を**スピングラス** (spin glass) と呼ぶ．

1973年，エドワーズ (Edwards) とアンダーソン (Anderson) は磁性の異なる複数の物質が十分混ざり合った後に急冷されたというスピングラスの特徴をなるべく簡単に表現するために最隣接相互作用に限定されたスピン対 $\langle ij\rangle$ の結合 $J_{\langle ij\rangle}$ がある同一の確率分布 $\mathcal{P}(J_{\langle ij\rangle})$ から選ばれると仮定したイジングスピンモデル，エドワーズ・アンダーソン (EA) モデルを提案した [2].

EAモデルではハミルトニアンがランダムに定まる結合 $\left\{J_{\langle ij\rangle}\right\}$ 毎に決まるため，各スピンの平均値 $\langle S_i\rangle$ もこの結合に依存したランダム変数となる．そのため $[\langle S_i\rangle]_J$，$\left[\langle S_i\rangle^2\right]_J$ などこの“ラン

[1]E-mail: kaba@dis.titech.ac.jp

ダムな平均値" に対するモーメントを求めることが必要となる．ただし，$[\ldots]_J$ は

$$[\cdots]_J \equiv \int \prod_{\langle ij \rangle} dJ_{\langle ij \rangle} \mathcal{P}\left(J_{\langle ij \rangle}\right)(\cdots) \tag{2}$$

で与えられるランダム結合 $\left\{J_{\langle ij \rangle}\right\}$ に関する平均を表し，ボルツマン分布による**熱平均** (thermal average)$\langle \ldots \rangle$ と区別して**配位平均** (configuration average) と呼ばれる．

スピングラスではボルツマン分布による通常の熱平均に加えて配位平均の評価が必要となり，強磁性体モデルにも増して解析が困難である．残念ながら，EA モデルも未だ厳密解は求められていない．そのような場合，解析の糸口として現象のからくりがガラス張りに分かる計算可能なモデルが果たす役割は大きい．そういった観点から 1975 年，シェリントン (Sherrington) とカークパトリック (Kirkpatrick) により EA モデルに対する平均場モデルが導入された [15]．これを彼らの名前の頭文字を取って SK モデルと呼ぶ．

SK モデルでは分配関数の解析計算がなるべく容易になるように強磁性体の平均場モデルと同じく各スピンは他のすべてのスピンと結合していると仮定してハミルトニアンを

$$\mathcal{H}(\boldsymbol{S}|\{J_{ij}\}) = -\sum_{i>j}\left(\frac{J_0}{N} + \frac{J_{ij}}{\sqrt{N}}\right) S_i S_j \tag{3}$$

で与える．ただし，$J_0 > 0$ は定数とし，やはり計算が容易になるように J_{ij} は平均ゼロ，分散が J^2 となるガウス分布

$$\mathcal{P}(J_{ij}) = \frac{1}{\sqrt{2\pi J^2}} \exp\left[-\frac{J_{ij}^2}{2J^2}\right] \tag{4}$$

で与えられるとする．J_0，J_{ij} がそれぞれ N，$\sqrt{N}$ で割られているのは他のスピンからの影響を大自由度極限 $N \to \infty$ で $\mathcal{O}(1)$ とするためである．

2.2 レプリカ法

まずはじめに，なぜ配位平均の評価が困難であるかについて述べておく．そのためには例えば $[\langle S_i \rangle]_J$ の定義式

$$[\langle S_i \rangle]_J = \int \prod_{\langle ij \rangle} dJ_{\langle ij \rangle} \mathcal{P}\left(J_{\langle ij \rangle}\right) \left(\frac{\mathrm{Tr}_{\boldsymbol{S}}\, S_i e^{-\beta \mathcal{H}(\boldsymbol{S}|\{J_{\langle ij \rangle}\})}}{\mathcal{Z}\left(\beta | \left\{J_{\langle ij \rangle}\right\}\right)}\right) \tag{5}$$

を検討してみるとよい．この定義式の $(\ldots)$ の中を見れば分かるように熱平均量の配位平均を計算する際には必ずランダム変数 $\left\{J_{\langle ij \rangle}\right\}$ に依存した分配関数 $\mathcal{Z}\left(\beta | \left\{J_{\langle ij \rangle}\right\}\right) = \mathrm{Tr}_{\boldsymbol{S}}\, e^{-\beta \mathcal{H}(\boldsymbol{S}|\{J_{\langle ij \rangle}\})}$ の逆数を含む量の平均評価が必要となる．一般にランダム変数の自然数冪を含む量の平均に関しては母関数の方法など比較的容易な系統的計算手法がある．しかしながら，逆数冪を含む量に関しては直接的な評価法以外に汎用性のある計算手法が知られておらず大自由度系に関してこれを行うことは非常に難しくなるのである．

スピングラス理論の標準的解析手法であるレプリカ法は分配関数の自然数冪に関する配位平均の結果を実数冪に解析接続することでこの困難を克服しようとする計算技法である．実のところ

この技法に関する数学的正当性は未だ証明されていない．にも関わらず，これまでにレプリカ法の操作自体が問題となって間違った結果が得られた例は知られていない．

式(5)の評価を具体例として述べる．$\mathcal{Z}\left(\beta|\left\{J_{\langle ij\rangle}\right\}\right)$ の逆冪を含んだ量の評価を避けるためまず一般の自然数 n に関して式(5)の代わりに

$$\begin{aligned}\left[\langle S_i\rangle\right]_{J,n} &\equiv \frac{\left[\mathcal{Z}^n\times\langle S_i\rangle\right]_J}{\left[\mathcal{Z}^n\right]_J}\\ &= \frac{\int\prod_{\langle ij\rangle}dJ_{\langle ij\rangle}\mathcal{P}\left(J_{\langle ij\rangle}\right)\left(\mathrm{Tr}_{\boldsymbol{S}^1,\ldots,\boldsymbol{S}^n}S_i^1 e^{-\beta\sum_{a=1}^n\mathcal{H}(\boldsymbol{S}^a)}\right)}{\int\prod_{\langle ij\rangle}dJ_{\langle ij\rangle}\mathcal{P}\left(J_{\langle ij\rangle}\right)\left(\mathrm{Tr}_{\boldsymbol{S}^1,\ldots,\boldsymbol{S}^n}e^{-\beta\sum_{a=1}^n\mathcal{H}(\boldsymbol{S}^a)}\right)}\end{aligned}\tag{6}$$

を求めておく．ただし，表記の簡略化のためハミルトニアン，分配関数に関する $J_{\langle ij\rangle}$ 依存性は省略して書いている．この量の分子は分配関数の自然数冪 $\mathcal{Z}^n$ を掛けてから配位平均を取っているため $n=1,2,\ldots$ に関しては逆冪の問題は起こらず，自然数 n の関数として求まる．その後，この関数が自然数の n のみでなく実数全体に関しても成立すると仮定し極限式

$$\left[\langle S_i\rangle\right]_J=\lim_{n\to 0}\left[\langle S_i\rangle\right]_{J,n}\tag{7}$$

を経由して配位平均を計算するのである．レプリカ法という名称は

$$\mathcal{Z}^n\left(\beta|\left\{J_{\langle ij\rangle}\right\}\right)=\mathop{\mathrm{Tr}}_{\boldsymbol{S}^1,\ldots,\boldsymbol{S}^n}\exp\left[-\beta\sum_{a=1}^n\mathcal{H}\left(\boldsymbol{S}^a|\left\{J_{\langle ij\rangle}\right\}\right)\right]\tag{8}$$

が同一のランダムネス $\left\{J_{\langle ij\rangle}\right\}$ を共有する n 個の複製系(レプリカ) $\left\{\boldsymbol{S}^1,\ldots,\boldsymbol{S}^n\right\}$ を一つの物理系とみなした際の分配関数を意味することに由来する．

大自由度極限 $N\to\infty$ では平均(6)は自由エネルギー $(1/nN)\ln\left[\mathcal{Z}^n\right]_J$ をレプリカ添字 $a,b=1,2,\ldots,n$ に依存する秩序変数に関して鞍点評価することで求められる．ただし，極限 $n\to 0$ を行うためには秩序変数のレプリカ添字に関する依存性に関し何らかの対称性を課す必要が生じる．ここで，これまでのところレプリカを区別する添字 $a,b=1,2,\ldots,n$ に関して計算は全て対称である．ということは，鞍点もこれらの添字に関し対称であると仮定することは尤もらしい．これをレプリカ対称(Replica Symmetric, RS)仮定，得られる解をレプリカ対称(RS)解と呼ぶ．

RS仮定の下，SK模型から導かれる自由エネルギーは

$$\begin{aligned}\frac{\ln\left[\mathcal{Z}^n\right]_J^{RS}}{nN} &= \mathop{\mathrm{Ext}}_{m,q,\widehat{m},\widehat{q}}\left\{-\frac{\beta J_0}{2}m^2-\frac{\beta^2J^2}{4}\left(1+(n-1)q^2\right)\right.\\ &+ \left.\frac{1}{n}\ln\left[\int Dz\left(2\cosh\left(\sqrt{\widehat{q}}z+\widehat{m}\right)\right)^n\right]-\widehat{m}m-\frac{(n-1)}{2}\widehat{q}q-\frac{1}{2}\widehat{q}\right\}\end{aligned}\tag{9}$$

となる．ただし，$Dz=\exp[-z^2/2]/\sqrt{2\pi}$ であり，$m=(1/N)\sum_{i=1}^N S_i^a$，$q=(1/N)\sum_{i=1}^N S_i^aS_i^b$ とした．$\mathrm{Ext}\{\cdots\}$ は鞍点評価を意味する．式(9)を見る限り，n が自然数である必要はなく実数への読み替え(解析接続)は容易である．$n\to 0$ に関し鞍点を取ることで秩序変数 m,q は求まる．また，各サイトに関するスピン平均のモーメントは鞍点における共役変数 $\widehat{m},\widehat{q}$ の値を用いて

$$\left[\langle S_i\rangle^k\langle S_j\rangle^l\right]_J=\int Dz_i\tanh^k\left(\sqrt{\widehat{q}}z_i+\widehat{m}\right)\times\int Dz_j\tanh^l\left(\sqrt{\widehat{q}}z_j+\widehat{m}\right)\tag{10}$$

(ただし，$k,l=0,1,2,\ldots$，$i\neq j$)のように評価されることが示される．

2.3 スピングラスとベイズ統計

実際のところ，RS解は低温において正しくないことが示されており，正しい解を求めるためにレプリカ対称性の破れた解をどう構成して行くか，というくだりがスピングラス理論における一つのハイライトである．しかしながら，以下の話題に関してこのことはさほど重要ではないのでここでは割愛する．興味のある方は文献[12]などを参考にして欲しい．

むしろここで強調しておきたいことはスピングラス理論とベイズ統計の類似性である．

2つの確率事象 A および B に関してそれらを記述する同時確率分布 $\mathcal{P}(A,B)$ が与えられているとしよう．ベイズ統計とは事象 A の観測値が与えられた際に事象 B についての条件つき確率(事後分布 (posterior distribution)) を与えるベイズ (Bayes) の公式

$$\mathcal{P}(B|A) = \frac{\mathcal{P}(A,B)}{\mathcal{P}(A)} = \frac{\mathcal{P}(A,B)}{\mathrm{Tr}_B\,\mathcal{P}(A,B)} = \frac{\mathcal{P}(A|B)\mathcal{P}(B)}{\mathrm{Tr}_B\,\mathcal{P}(A|B)\mathcal{P}(B)} \tag{11}$$

を用いて，未観測事象 B に関する効率的な予測・推定を行う統計学の枠組である．高校の確率・統計にも登場する基礎的な公式であるだけに，統計性を伴う情報処理においてベイズ統計の枠組で定式化される問題は多い．例えば，過去の天気を A，明日の天気を B に対応させれば気象に関するある確率モデル $\mathcal{P}(A,B)$ に基づき天気予報をする問題はまさにこの枠組で表現されるし，次節に登場する情報通信に関する問題の多くもこの枠組で定式化出来る．

ベイズ統計の枠組には様々な状況下での予測法を見通し良く書き下すことが出来るという利点がある．その際，得られた予測法は実際に期待値としてどの位有用であるのか，という性能評価の問題は理論的にも実用面からも重要である．ベイズ統計を用いた予測法は一般に事後分布に関する予測値 B の様々な平均量に基づいて構成される．そのため，その平均的な性能を評価するためには B の事後分布による平均を更に観測値 A に関して平均化する必要がある．ただし，このような2重の平均操作は特殊な場合を除き非常に複雑であり，多くの問題で必要とされる割に，系統的な計算方法はほとんど知られていない．

ところが，本節で取り上げたスピングラスモデルではレプリカ法を使ってまさにこの2重の平均操作を行っていたことに注意しよう．$\{J_{ij}\} \to A$，$S \to B$，ボルツマン分布 $\to$ 事後分布 と対応させればスピングラスの問題とはベイズ統計における平均性能評価問題に他ならないのである．ただし，本来合金の磁性を調べる問題として出発したために平均場モデル (SK模型) による解析という，一般のベイズ統計ではあまり馴染みのない接近法が導入されたのであった．この接近法とレプリカ法を組み合わせることでベイズ統計で定式化される多くの情報処理の問題に関してこれまでにない汎用的で系統的な性能評価法が与えられる可能性がある．

連想記憶模型への応用がなされた80年代中頃にはまだこのような意識は希薄であった[1]．しかしながら，90年代に学習理論との関わりを持った[20]ことで多くの研究者に認識されはじめ，現在ベイズ統計による定式化を利用したスピングラス理論の体系的な応用ともいうべき分野が確実に広まりつつある[4]．

3 誤り訂正符号の枠組

情報通信に関する普遍的な問題の一つに伝送路を経由する際に熱雑音等が原因で生じる誤りがある．そこで，信頼性の高い通信を行うためには仮に誤りが生じてもそれを訂正出来るような仕組みを考えておく必要がある．

この問題を数学的に定式化し，定量的に議論する枠組を与えたのが情報通信理論の開祖シャノン (Shannon) である [14]．通常，情報は各成分が $0,1$ あるいは ± 1 の2値で表される N ビットベクトル $\boldsymbol{\xi} = (\xi_1, \xi_2, \ldots, \xi_N)$ $(\xi_i = 0, 1, \text{or} \pm 1,\ i = 1, 2, \ldots, N)$ のように表現される．以下，$0,1$ による表現を2進数表現，± 1 による表現をイジングスピン表現と呼ぶことにする．

シャノンによると誤りを訂正する仕組みを作るためには原情報 $\boldsymbol{\xi}$ をそれより長い $M(> N)$ ビットの長さを持つ**符号語** $\boldsymbol{J}^0$ と呼ばれるベクトルに一旦変換 (**符号化** (encode)) してから送信すればよい．実際には N ビットで表現できる情報をわざわざそれより長い M ビットに直して送信するのだから冗長である．受信者は仮に誤りを含む符号語を受け取ったとしてもこの冗長性を手掛かりにして原情報を復元 (**復号** (decode)) できる．このように情報表現に冗長な符号化を行うことによって誤りを訂正する技術を一般に**誤り訂正符号** (error-correcting codes) と呼ぶ．

信頼性の高い通信を行うためには誤りが生じる確率を出来るだけ小さくしたい．そのためには誤り訂正の手掛かりとなる冗長性はなるべく沢山ある方が良い．しかしながら，単位時間当たりに送信出来るビット数は一定である．通信時間などのコストを考慮すれば符号語1ビット当たりに含まれる原情報の情報量を表す符号化率 $R = N/M$ を大きく，つまり冗長性はなるべく少なくすることが望まれる．誤り訂正符号の開発研究ではこの相反する2つの要請を出来るだけ満足するような符号化/復号法の設計が求められる．

これに対しシャノンは以下のような符号の限界性能に関する定理も与えている．

Theorem 1 (通信路符号化定理) 原情報，符号語のビット長をそれぞれ N，M とする．反転確率 p の2値対称通信路に対し，$N, M \to \infty$ の極限では符号化率 $R = N/M$ が

$$R < 1 - H_2(p) \tag{12}$$

ただし，

$$H_2(p) \equiv -p \log_2 p - (1-p) \log_2 (1-p) \tag{13}$$

ならば通信により生じる誤りを限りなくゼロに近くする符号化法が存在する．

逆に $R > 1 - H_2(p)$ では絶対に誤り確率をゼロに出来ないことも示される．また，他の通信路モデルについても同様の定理が示される．不等式 (12) の右辺はしばしばシャノン極限と呼ばれる．

残念ながら，通信路符号化定理は存在定理であり効率的な誤り訂正符号を研究してきた情報/符号理論においてもシャノン極限を達成する実用的符号の構成法は未だ知られていない．

4 低密度パリティ検査符号とスピングラスモデル

情報/符号理論ではあまり強調されないが，実のところ誤り訂正符号はベイズ統計そのものである．原情報は事前確率 $\mathcal{P}(\boldsymbol{\xi})$ から発生するとしよう．また，伝送路でのノイズは符号語 $\boldsymbol{J}^0(\boldsymbol{\xi})$ を送

信した条件下で受信者が受信ベクトル $\boldsymbol{J}$ を受け取る条件付き確率 $\mathcal{P}\left(\boldsymbol{J}|\boldsymbol{J}^0(\boldsymbol{\xi})\right)$ で表現される．ただし，符号語は原情報の関数であることを強調するため $\boldsymbol{J}^0(\boldsymbol{\xi})$ と表した．すると，$\boldsymbol{J}$ を受け取った後，原情報に関する事後分布は

$$\mathcal{P}(\boldsymbol{S}|\boldsymbol{J}) = \frac{\mathcal{P}\left(\boldsymbol{J}|\boldsymbol{J}^0(\boldsymbol{S})\right)\mathcal{P}(\boldsymbol{S})}{\mathcal{Z}(\boldsymbol{J})} \tag{14}$$

となる．ここで，$\mathcal{Z}(\boldsymbol{J}) = \mathrm{Tr}_{\boldsymbol{S}}\,\mathcal{P}\left(\boldsymbol{J}|\boldsymbol{J}^0(\boldsymbol{S})\right)\mathcal{P}(\boldsymbol{S})$ は分配関数に対応する規格化定数である．

事後分布 (14) が与えられると，目的に応じた最適戦略を系統的に求めることが出来る．例えば，原情報 $\boldsymbol{\xi}$ とその推定値 $\widehat{\boldsymbol{\xi}}$ が完全に同一になる確率を最大化したければ $\widehat{\boldsymbol{\xi}} = \mathrm{argmax}_{\boldsymbol{S}}\{\mathcal{P}(\boldsymbol{S}|\boldsymbol{J})\}$ とすればよい．また，ビット毎の誤り確率を最小にしたければ各ビットに対し周辺分布 $\mathcal{P}(S_i|\boldsymbol{J}) = \mathrm{Tr}_{\boldsymbol{S}/S_i}\mathcal{P}(\boldsymbol{S}|\boldsymbol{J})$ を計算し偏っている方のビット値を推定値とすればよい．

さて，従来ベイズ統計による定式化はこのような最適戦略を導く議論に終始していた．ところが

$$\mathcal{H}(\boldsymbol{S}|\boldsymbol{J}) = -\ln\left[\mathcal{P}\left(\boldsymbol{J}|\boldsymbol{J}^0(\boldsymbol{S})\right)\mathcal{P}(\boldsymbol{S})\right] \tag{15}$$

とすれば，これらの方策はそれぞれ温度 $T=0$，$T=1$ (西森温度)[11] でのボルツマン分布を用いた推定に他ならない．また，ランダムに与えられる $\boldsymbol{J}$ から定まるボルツマン分布という構造はスピングラスと共通するものであり，レプリカ法を導入することで性能評価が可能になる．

以下，低密度パリティ検査符号と称される符号族の一種であるソウラス (Sourlas) 符号 [16, 5] と MN(マッカイ (MacKay)・ニール (Neal)) 符号 [10, 7] に関する解析結果を述べる．

4.1 ソウラス符号

イジングスピン表現を用いた場合，この符号では原情報 $\boldsymbol{\xi}$ に対し，ランダムに選ばれた $K(\geq 2)$ 個の成分の積

$$J^0_\mu = \xi_{l_{\mu,1}}\xi_{l_{\mu,2}}\ldots\xi_{l_{\mu.K}},\ (\mu = 1,2,\ldots,M) \tag{16}$$

により符号語 $\boldsymbol{J}^0$ を構成する．また，情報伝達効率の偏りをなくすため，各ビットはなるべく公平に符号構成に用いられるとする．添字 $l_{\mu,i}$ は符号語の第 $\mu(=1,2,\ldots,M)$ 成分を構成する K 個の原情報の要素のうち $i(=1,2,\ldots,K)$ 番目の成分を表す．これはスピングラス研究で知られているマチス (Mattis) モデルにおける結合定数の与え方と同じである．

$\{+1,-1,\times\}\to\{0,1,+\}$ によりイジングスピン表現から 2 進数表現に変換するとこの符号化は，各行に関し非ゼロ (1) の要素数は K 個という拘束条件の下でランダムに構成された 2 進数上の $M\times N$ 次元疎行列 C_s による 2 進数上の線形変換 $\boldsymbol{J}^0 = C_s\boldsymbol{\xi}\ (\mathrm{mod}\ 2)$ に他ならない．

再びイジングスピン表現に戻ると，事後分布に対応するハミルトニアンは

$$\mathcal{H}(\boldsymbol{S}|\boldsymbol{J}) = -F_n\sum_{\mu=1}^{M}J_\mu S_{l_{\mu,1}}S_{l_{\mu.2}}\ldots S_{l_{\mu.K}} - F_s\sum_{l=1}^{N}S_l \tag{17}$$

となる．ただし，$J_{\mu=1,2,\ldots,M}$ は受信された系列であり符号語 (16) にノイズが加わったものである．ここで，$F_n = (1/2)\ln[(1-p)/p]$ はノイズの大きさを表し，F_s は原情報が各ビット独立な事前確率を持つ場合に対応するために導入した定数であり偏りがない場合にはゼロとなる．

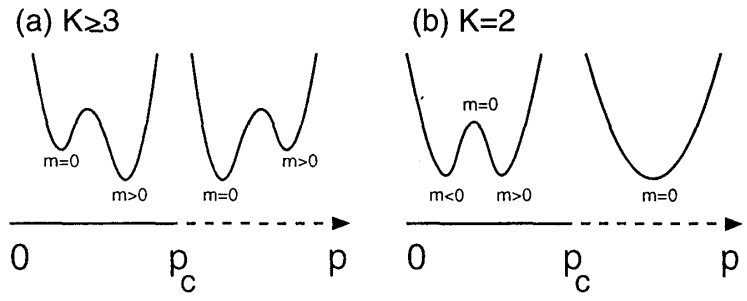

図 1: 原情報に偏りがない場合 ($F_s = 0$) に温度 $T \leq 1$ に対してレプリカ法から示される自由エネルギー眺望の概形. m は原情報と復号結果との重なり. (a)$K \geq 3$ の符号ではノイズレベル p がどのような値であっても $m > 0$(復号成功) および $m = 0$(復号失敗) で特徴付けられる 2 つの局所最小解が存在する. p がある臨界値 p_c より小さい場合には成功解が失敗解より低い自由エネルギーを持ち, 熱力学的に安定な解となる. ただし, この解の引き込み領域は失敗解と比較して狭く平均場近似法など自由エネルギーを降下させる工学的局所探索法によって現実的な時間で探索することは一般に困難である. $K \to \infty$ の場合, 成功解に関しては $m \to 1$, $p_c \to H_2^{-1}(1-R)$ となりシャノン極限を達成することが示される. 同時に成功解への引き込み領域の大きさは $\mathcal{O}(K^{-1})$ で減少する. (b)$K = 2$ の符号では, ある臨界値 p_c 以下のノイズでは復号成功解 $m > 0$ とその鏡像のみが自由エネルギーの最小解となる. 従って, どのような初期条件を与えても自由エネルギーを降下させる局所探索法を用いて成功解を探索することは容易である.

さて, 復号問題はランダム性が凍結された i) 原情報 $\boldsymbol{\xi}$, ii) 符号化法 C_s に依存するハミルトニアンで記述されるため性能評価にはスピングラスと同様 $\boldsymbol{S}$ に関する熱平均に加えて $\boldsymbol{\xi}, C_s$ に関する配位平均が必要となる. レプリカ法を導入することでこの 2 重平均操作は可能となる. ただし, 1 スピンあたりに結合しているスピン数が $\mathcal{O}(1)$ の希釈模型であるため必要な計算はかなり繁雑になる [5]. レプリカ法により得られた定性的な結果のみを図 1に示す.

4.2 MN 符号

MN 符号では C_s に加え各行・各列あたり非ゼロ (1) の要素数が $L(\geq 2)$ となる拘束条件下でランダムに生成された 2 進数上の $M \times M$ 可逆疎行列 C_n を導入して符号を構成する[2].

2 進数表現を用いると符号化は 2 つの行列 C_s, C_n を用いて $\boldsymbol{z}^0 = C_n^{-1} C_s \boldsymbol{\xi} \pmod 2$ により行われる. 送信後, $\boldsymbol{z}^0$ ではなく受信者は M ビットのノイズベクトル $\boldsymbol{\zeta}$ が加わった符号語

$$\boldsymbol{z} = \boldsymbol{z}^0 + \boldsymbol{\zeta} = C_n^{-1} C_s \boldsymbol{\xi} + \boldsymbol{\zeta} \pmod 2 \tag{18}$$

を受信する. 復号とは $\boldsymbol{z}$ から $\boldsymbol{\xi}$ を推定する作業である. MN 符号ではこのために直接式 (18) を用いるのではなく, これに左から C_n を掛けて得られる方程式

$$\boldsymbol{J} = C_n \boldsymbol{z} = C_s \boldsymbol{S} + C_n \boldsymbol{\tau} \pmod 2 \tag{19}$$

[2] $L = 1$ の場合はソウラス符号に帰着する.

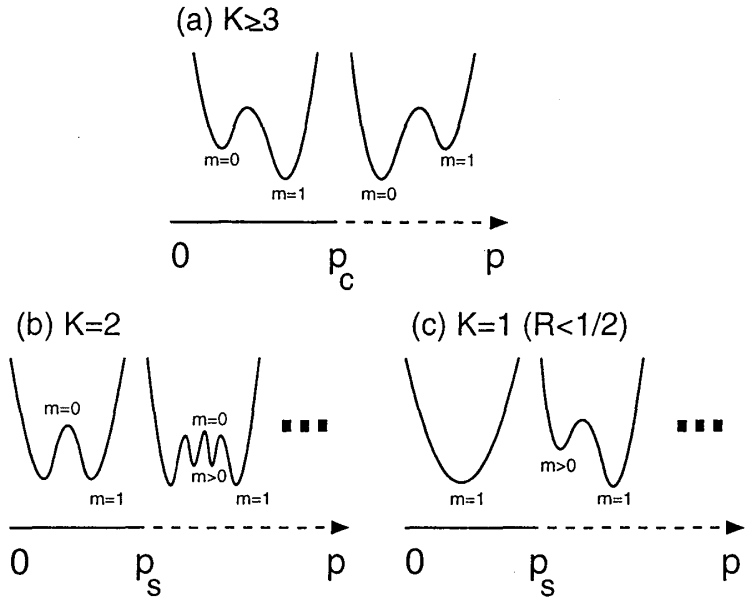

図 2: 原情報に偏りがない場合 ($F_s = 0$) に温度 $T \leq 1$ に対してレプリカ法から示される自由エネルギー自由エネルギー眺望の概形. m は原情報と復号結果との重なり. (a)$K \geq 3$ の符号ではノイズレベル p がどのような値であっても $m = 1$(復号成功) および $m = 0$(復号失敗) で特徴付けられる 2 つの局所最小解が存在する. p がシャノン極限 $p_c = H_2^{-1}(1-R)$ より小さい場合には成功解が失敗解より低い自由エネルギーを持ち, 熱力学的実現される解となる. すなわち, シャノン極限を達成する. ただし, 局所探索法による成功解の探索は困難である. (b)$K = 2$, (c)$K = 1$ $(R < 1/2)$ の符号では, スピノーダル点 p_s 以下のノイズでは復号成功解 $m = 1$ とその鏡像のみが自由エネルギーの最小解となる. 従って, どのような初期条件を与えても自由エネルギーを降下させる局所探索法を用いて成功解を探索することは容易である.

を未知変数 $\boldsymbol{S}$, $\boldsymbol{\tau}$ に関して解くことで行う. 得られた $\boldsymbol{S}$, $\boldsymbol{\tau}$ がそれぞれ $\boldsymbol{\xi}$, $\boldsymbol{\zeta}$ の推定値である.

方程式 (19) と統計的拘束条件を融合するためにはやはりベイズ統計の形式を用いるのが便利である. イジングスピン表現を導入すると方程式 (19) に対応するハミルトニアンは

$$\mathcal{H}(\boldsymbol{S}, \boldsymbol{\tau} | \boldsymbol{J}) = \gamma \sum_{\mu=1}^{M} \frac{1 - J_\mu \prod_{l \in \mathcal{L}_s(\mu)} S_l \prod_{j \in \mathcal{L}_n(\mu)} \tau_j}{2} - F_s \sum_{l=1}^{N} S_l - F_n \sum_{j=1}^{M} \tau_j \tag{20}$$

となる. ただし, $\mathcal{L}_s(\mu)$, $\mathcal{L}_n(\mu)$ はそれぞれ J_μ に関連するスピン変数 S_l, τ_j の添字の集合, F_s は原情報の偏りを表し, $F_n = (1/2)\ln[(1-p)/p]$ である. 真の事後確率は温度 $T = 1$, $\gamma \to \infty$ に対応する. この符号の性能もソウラス符号同様レプリカ法により求めることが出来る [7]. 図 2に定性的な結果を示す.

4.3 公開鍵暗号への応用

公開鍵暗号とは暗号鍵 (公開鍵) と復号鍵 (秘密鍵) を分離することにより, 秘密漏洩の危険性について秘密鍵保持者のみで管理することを可能にした暗号方式である. ソウラス符号と MN 符

号の関係を利用すると公開鍵暗号の一例を具体的に構成することができる [8].

以下，平文 $\boldsymbol{\xi}$ は2進数ベクトルで表現されているものとする．ソウラス/MN 符号を用いた公開鍵暗号では MN 符号で用いられる疎行列 C_s，C_n に加えて可逆な密行列 D を導入し

$$K_p = (C_n^{-1} C_s D, p) \tag{21}$$

を公開鍵とする．ただし，p はノイズの生成確率を表し，局所探索法による実時間復号が可能であるように C_s，C_n，p は選ばれているものとする．一方，これに対する秘密鍵は

$$K_s = (C_n, D) \tag{22}$$

である．密行列 D の導入は公開鍵から秘密鍵の情報が漏洩する可能性を防ぐためである．

暗号化は式 (18) と同様

$$\boldsymbol{z} = C_n^{-1} C_s D \boldsymbol{\xi} + \boldsymbol{\zeta} \pmod 2 \tag{23}$$

により行う．ただし，$\boldsymbol{\zeta}$ は安全性を確保するためビット毎に確率 p で1を生成した2進数ノイズベクトルである．

復号はまず暗号文 (23) に左から C_n を掛け MN 符号の場合と同様に局所探索法を用いて $D\boldsymbol{\xi}$ を求める．その後，D^{-1} を作用させ平文 $\boldsymbol{\xi}$ を求めれば良い．

最後にこの暗号の安全性に関し簡単に触れておこう．まず，公開鍵 K_p から秘密鍵 K_s が見破られる危険性であるが $C_n^{-1} C_s D$ が与えられた際にこれを2つの疎行列と1つの密行列に分解する問題は一般に計算量的に困難であることが知られている．

次に公開鍵 K_p を用いた復号の可能性を考えよう．ここで，$C_n^{-1} C_s D$ は各行あたりの非ゼロ要素数が $\mathcal{O}(N)$ である密行列であることに着目しよう．これは $K \to \infty$ におけるソウラス 符号の復号問題に対応している．ソウラス符号の性質として復号成功相への局所探索法の引き込み領域の大きさは $K \to \infty$ の極限で $\mathcal{O}(K^{-1})$ で減少する．そのため，ほぼ完全に平文 $\boldsymbol{\xi}$ の情報が事前に得られていない限り局所探索法による実時間での復号は絶望的である．

5 今後の可能性について

本稿ではスピングラス理論の誤り訂正符号及び暗号への応用について述べた．しかしながら，本文中で触れた通りスピングラス理論の形式はベイズ統計のそれとほぼ同じである．情報通信技術の発達により大規模なベイズ統計モデルで定式化され得る問題は増加している．誤り訂正符号，公開鍵暗号，画像修復 [17, 13] といった比較的単純な技術だけではなく今後は各種通信プロトコルやネットワーク通信 [18] などの高度な情報通信技術へも展開されていくと思われる．

また，今回はレプリカ法を使った性能評価に焦点を絞って述べた．しかしながら，工学では性能評価といった巨視的な物の見方だけでなく如何にそれを達成する解を求めるか，という微視的な解析に対応したアルゴリズム開発も重要である．最近ではこの問題に関し統計力学における平均場近似を応用する研究が始まっている．実際，ここで述べたソウラス符号や MN 符号の復号にもスピングラス理論で知られている TAP の方法 [19] を高性能な近似的復号アルゴリズムとして

利用することが出来る [6]. この方向性はレプリカ法の応用と比較して始まってからまだ日が浅く今後の発展が期待されている.

従来, 情報通信の理論は専ら情報/符号理論として発展してきた. 当然, それらとスピングラス理論との関係を明らかにすることは興味深い [3, 9]. 従来の情報/符号理論は数学的に厳密な議論に基づいている. このような方向性はレプリカ法の数学的基礎付けにもつながると考えられる.

参考文献

[1] DJ. Amit, H. Gutfreund and H. Sompolinsky, Phys. Rev. Lett. **55**, 1530, 1985.

[2] SF. Edwards and PW. Anderson. J. Phys. **F 5**, 965, 1975.

[3] 伊庭幸人. 情報理論における Gallager formalism とレプリカ法, 未公開, 1989.

[4] 樺島祥介. 岩波講座 物理の世界 「学習と情報の平均場理論」, 出版予定 (岩波書店), 2001.

[5] Y. Kabashima and D. Saad. Europhys. Lett. **44**, 668, 1998.

[6] Y. Kabashima and D. Saad. Europhys. Lett. **45**, 97, 1999.

[7] Y. Kabashima, T. Murayama and D. Saad. Phys. Rev. Lett. **84**, 1355, 2000.; 村山立人, 物性研究 **72** No. 6, 876, 1999.

[8] Y. Kabashima, T. Murayama and D. Saad. Phys. Rev. Lett. **84**, 2030, 2000.

[9] Y. Kabashima, N. Sazuka, K. Nakamura and D. Saad. cond-mat/0010173, 2000.

[10] DJC. MacKay. IEEE Trans. on IT **45**, 399, 1999.

[11] H. Nishimori. Prog. Theor. Phys. **69**, 1169, 1981.; J. Phys. Soc. Jpn. **62**, 2793, 1993.

[12] 西森秀稔. 新物理学選書 「スピングラス理論と情報統計力学」, 岩波書店, 1999.

[13] H. Nishimori and KYM. Wong, Phys. Rev. E **60**, 132, 1999.

[14] CE. Shannon. Bell. Sys. Tech. J. **27**, 379, 1948.; **27**, 623, 1948.

[15] D. Sherrington and S. Kirkpatrik. Phys. Rev. Lett. **35**, 1792, 1975.

[16] N. Sourlas. Nature **339**, 693, 1989.

[17] 田中和之. 日本物理学会誌 **54**, 25, 1999.

[18] T. Tanaka. "Statistical mechanics of cdma multiuser demodulation", to appear in Europhys. Lett., 2001.

[19] DJ. Thouless, PW. Anderson and RG. Palmer. Phil. Mag. **35**, 593, 1977.

[20] TLH. Watkin, A. Rau and M. Biehl. Rev. Mod. Phys. **65**, 499, 1993.